

МАТЕМАТИЧНИЙ ІНСТРУМЕНТАРІЙ ДЛЯ АНАЛІЗУ ІНТЕРНЕТУ РЕЧЕЙ

Анотація. Наведено огляд публікацій останніх років щодо використання математичних методів та моделей для аналізу інтернету речей. Відзначено, що під час моделювання інтернету речей використовують такі розділи математики, як теорія ігор, теорія ймовірностей, теорія випадкових процесів, булева та матрична алгебри, теорія графів, теорія чисел, теорія функцій комплексної змінної, теорія міри, теорія оптимізації, імітаційне моделювання, кластерний аналіз, чисельний аналіз, математичний аналіз.

Ключові слова: інтернет речей, методи, моделі, моделювання, технології, структура, система.

Останнім часом термін «інтернет речей» (Internet of Things, IoT) дуже широко використовують не лише фахівці з інформаційних технологій, а також у повсякденному житті.

Термін IoT вперше був введений британським дослідником та підприємцем Кевіном Ештоном. Наприкінці 90-х років Ештон вивчав радіочастотну ідентифікацію (RFID). За цією технологією на предмети закріплюють маленькі датчики (сенсори), що містять важливу інформацію і дозволяють зчитувати її на відстані за допомогою мережі Інтернет. Ештон запровадив цей термін, щоб проілюструвати можливості RFID, які використовують в корпоративних системах постачання. Одна із задач полягала у тому, щоб рахувати товари і відстежувати їхнє пересування без людського втручання. Сьогодні термін IoT став найбільш вживаним для опису сценаріїв, у яких інтернет-з'єднання та обчислювальна здатність поширюються на безліч об'єктів, пристроїв і сенсорів.

Нині терміном IoT позначають мережу, що складається із взаємозв'язаних фізичних об'єктів або пристроїв, які мають вбудовані сенсори. Також його асоціюють з програмним забезпеченням, що дозволяє з використанням стандартних протоколів зв'язку здійснювати передачу та обмін даними між фізичним світом і комп'ютерними системами. Крім сенсорів, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і з'єднані між собою через дротові та бездротові мережі. Ці взаємоз'єднані об'єкти мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також унеможливають участь людини, використовуючи інтелектуальні інтерфейси.

Проаналізувати особливості моделювання та реалізації технологій IoT, а також основні технічні характеристики пристроїв, які застосовують, неможливо без використання математичних методів і моделей програмування.

У наукових доробках вітчизняних та зарубіжних учених, теоретиків та практиків, що досліджують IoT, послуговуються певним математичним апаратом. Науковці лише в останньому десятилітті почали активно аналізувати роботу IoT та застосовувати для цього широкий спектр математичних методів та моделей. Заслугове на увагу систематизація вказаних методів і моделей для аналізу математичного апарату, що використовують для моделювання роботи технологій IoT.

Систему фізичної безпеки об'єкту інфраструктури регіону на основі функціонування технологій IoT розглянуто в [1]. Тут використано теоретико-множинну модель функцій, компонентів і відмов досліджуваної системи, а та-

кож показано проекцію ієрархічної структури відмов основних структурних елементів системи фізичної безпеки. Діаграма IDEF0 — методологія функціонального моделювання (function modeling) і графічна нотація — призначена для формалізації та опису бізнес-процесів і показує сценарій випадкового або навмисного відключення електричного живлення у зв'язку підсистем освітлення і відеоспостереження. У цій роботі розроблено моделі і методи аналізу ризиків систем фізичної безпеки.

У [2] стверджують, що в процесі забезпечення інноваційного розвитку підприємств машинобудування в концепції Індустрії 4.0 необхідно використовувати математичні моделі, які будуть відповідати технологіям машинного зору, роботизованої техніки, автоматизованих та інтелектуальних систем виробництва й керування в рамках кіберфізичних систем на підприємствах. На думку авторів [2], такі кіберфізичні системи мають бути пов'язані із зовнішнім світом через сенсори і виконавчі механізми, що дозволяють отримувати потоки даних із фізичного світу, встановлювати і безперервно оновлювати віртуального близнюка фізичного світу і забезпечувати взаємодію в реальності за інструкцією з віртуальної сфери. Наведені в роботі класи математичних моделей для кіберфізичних систем запропоновано використовувати відповідно до інновацій на машинобудівних підприємствах. Це забезпечить автоматизацію ручної праці, оновлення вже використаних інноваційних технологій та їхнє об'єднання в єдиному інформаційному просторі.

Основною проблемою, з якою зіткнулися під час розроблення застосовних програм для інтернету речей, є оптимальне використання енергетичних ресурсів, зокрема термін придатності батарей IoT. Методику, яку запропонували науковці з Греції [3], застосовано для аналізу характеристик параметрів, що впливають на споживання енергії, та для перевірки енергоспоживання пристроїв IoT. Особливі вимоги висувають і до енергоефективності системи (наприклад, термін експлуатації системи керування будівництвом). Такий підхід дозволяє деталізувати формальне уявлення про поведінку системи та її подальшу перевірку, чим забезпечує зворотний зв'язок для вдосконалення на етапах перед розгортанням або безпосереднім виробництвом.

Вузькосмуговий інтернет речей (NB-IoT) — це перспективна технологія низькопотужної мережі (LPWN), стандартизована проектом партнерства третього покоління (3GPP) release-13 як частина майбутнього п'ятого покоління (5G) системи бездротового зв'язку. Основною метою розробки NB-IoT було посилення радіопокриття повторенням сигналу впродовж додаткового періоду часу. В [4] наведено короткий огляд технології NB-IoT, зокрема варіанти розгортання, фізичні канали та сигнали, структура сітки ресурсів висхідної лінії і конфігурація ресурсних одиниць. У цій роботі розроблено модель системи для висхідної лінії зв'язку NB-IoT на основі специфікацій 3GPP release-13. Також було досліджено ефективність запропонованих NDMRS-допоміжних оцінювачів каналів у порівнянні з іншими за допомогою розлогого комп'ютерного моделювання на рівні каналів.

Доцільність використання платформи керування на основі IoT для надання даних зворотного зв'язку в реальному часі було досліджено в [5]. На думку авторів, це підвищить ефективність використання спектра та споживання енергії створенням мережі мовлення з адаптивною випромінювальною потужністю. У цій роботі представлено архітектуру мережі, яка включає контур зворотного зв'язку IoT. Ця мережа розроблена та оптимізована, що забезпечує мінімальне споживання електроенергії та ефективну інфраструктуру. Крім того, для оцінки покращення використання спектра запропоновано новий показник його ефективності.

У часи розвитку технологій, коли необхідно з'єднання між комп'ютерами, інтернет речей і різні застосовні програми, засновані на IoT, ефективніші за бездротову сенсорну мережу. На думку авторів [6], бурхливий розвиток технологій взагалі та IoT зокрема вимагає ефективного використання енергії та засобів зв'язку. Взаємодія між різними приладами на різних рівнях потребує групування та використання кластерного підходу. Автори представили прагматичну архітектуру IoT і запропонували два алгоритми кластеризації: на основі евристичного та графічного підходів, які дозволяють здійснювати кластеризацію у напрямку знизу до гори та зверху вниз залежно від необхідності застосування IoT. Алгоритми оцінюють за допомогою низки стандартних параметрів і порівнюють з існуючими алгоритмами, а багаторівнева структура IoT забезпечує ієрархічну структуру для ефективного підключення.

Грунтовний аналіз трафіку «розумних» пристроїв, застосованих під час розроблення інтелектуальних систем, було проведено в [7], де виявлено істотні відмінності в основних характеристиках трафіку однотипних пристроїв різних виробників. У цій роботі зазначено відсутність загальноприйнятих норм побудови інтелектуальних мереж та у деяких режимах їхнього функціонування показано неможливість прогнозування стрибків трафіку, що істотно ускладнює моделювання інтелектуальної системи. Автори вказали на необхідність поглибленого аналізу отриманих даних, який дасть повніше уявлення про функціонування розглянутих пристроїв та доцільність побудови імітаційної моделі мережі пристроїв IoT з подальшим ускладненням і збільшенням кількості вузлів.

Сучасні підходи до створення єдиного інформаційного простору промислових комплексів для визначення методології, яка дозволить більш повно розглянути інформаційно-комунікаційні зв'язки моделюючих систем, наведено в [8]. На основі методології SADT (Structured Analysis and Design Techniques) розроблено інформаційну IDEF0-модель розвитку смарт-підприємств, яка дозволить, на думку авторів, отримати повне уявлення про відповідні процеси. Зауважимо, що за згаданим підходом розглянуто логічні відносини між роботами, а не їхня послідовність у часі.

Група дослідників у [9], зробивши аналіз застосування IoT, вказала на значні проблеми, пов'язані з конфіденційністю. Це, на думку авторів, призводить до втрати контролю за збиранням і передаванням даних. Конфіденційність є основною вимогою в будь-якій екосистемі IoT і її порушення гальмує широке застосування інтернету речей. По-перше, автори оцінюють проблему конфіденційності в системах IoT і висловлюють занепокоєння через обмеження ресурсів, зокрема особистих даних, які безпосередньо передаються від сенсорів до зовнішнього світу. По-друге, описують запропоновані рішення IoT, які охоплюють різні проблемні аспекти конфіденційності, такі як ідентифікація, відстеження, моніторинг і профілювання. Автори розглядають механізми та архітектури для захисту даних IoT у разі мобільності пристрою, а також для інфраструктури платформного та прикладного рівней [9].

Дослідники з Греції [10] розглянули наявні мережеві комунікаційні технології для IoT, звертаючи увагу на протоколи інкапсуляції та маршрутизації. У роботі також досліджено взаємозв'язок між мережевими протоколами IoT і новими його застосовними програмами. Запропоновано ретельну таксономію протоколів на основі шарів мережі, в той час як мережеві протоколи придатні і працюють для адресації.

Дослідження програмного забезпечення для розроблення інтелектуальної системи охорони здоров'я на основі IoT проведено в [11]. На підставі різних технологічних стандартів і протоколів зв'язку проаналізовано вимоги до системи

IoT, що є основою для розроблення відповідних платформ. Запропонована модель складається з трьох рівнів, і на кожному виконується спеціалізована задача. Автори впевнені у дієвості інтелектуальних служб охорони здоров'я особливо у слаборозвинутих країнах та у сільській місцевості.

Архітектуру, яка є базою для розроблення легких мікросервісів на основі соціально пов'язаних вебоб'єктів для реалізації послуг SIoT (Social Internet of Things), досліджено в [12]. В запропонованій роботі проаналізовано модель соціальних відносин, що дає можливість ефективного виявлення вебоб'єктів і дозволяє зменшити складність надання послуг. Модель семантичної онтології розроблено для реалізації сумісної соціальної взаємодії між гетерогенними об'єктами.

У 2016 р. Європейський парламент ухвалив документ «Загальне положення про захист даних» (General Data Protection Regulation, GDPR), який безпосередньо стосується IoT в частині безпеки та конфіденційності даних користувачів. У [13] проаналізовано процес обробки IoT особистої інформації та досліджено безпосередній вплив GDPR на IoT. З огляду на GDPR, використовуючи модель Гордона та Лоеба, проаналізовано економічний вплив галузі IoT на вартість фірм. Також досліджено, які саме галузі є вразливими щодо вказаних законодавчих змін.

Нову автономну структуру безпеки, що представлено ефективною системою фільтрації мережевого трафіку для віртуалізованих та багатозадачних мереж NB-IoT з підтримкою 5G, описано в [14]. У цій роботі стверджують, що запропонована структура безпеки та система фільтрації можуть значно пом'якшити атаки за рахунок динамічного згортання та завантаження тисяч правил фільтрації у Firewall, що мають відповідну кількість пристроїв NB-IoT.

Сучасні проблеми безпеки в мережі IoT та їхню класифікацію розглянуто в [15]. Тут більш детально досліджено питання забезпечення конфіденційності, легких криптографічних структур, безпечних маршрутизації та пересилання, надійності та стійкості керування, відмови в обслуговуванні та виявлення інсайдерської атаки. На думку авторів, конфіденційність має вирішальне значення в IoT, оскільки характеристики такої мережі суттєво відрізняються від типової мережі Інтернет. У цій роботі запропоновано використовувати таку технологію візуалізації, як Software defined networking (SDN) — програмно-визначена мережа. Використання SDN передбачає централізацію моніторингу мережі, що у свою чергу забезпечить узгоджене надання послуг.

У [16] розглянуто такі моделі оцінки ймовірно-часових характеристик інформаційної взаємодії в мережі інтернету речей: імітаційна модель інформаційної взаємодії в інтренеті речей, яка заснована на мультиагентному підході; моделі доступу в «туманних обчисленнях» з дозволом колізій джерел даних в тимчасовій області, які реалізують відповідно режими опитування, переривань, множинного доступу. Запропоновані моделі можна використовувати на початкових етапах проєктування IoT.

Розширюючи доступність Інтернету через зондування та автоматизацію, мережеві взаємодії стають критичнішими і безпечнішими та потребують покращених засобів безпеки для проєктування та тестування компонентів системи, платформ та послуг. Через такі мережі проходить безліч безладних, різномірних даних. У [17] стверджують, що теорія категорій — галузі абстрактної математики — забезпечує концептуальну основу для інформаційного моделювання IoT.

Під час розроблення бездротових сенсорів і середовищ для багатьох прикладних областей (наприклад, екологічних, медичних, «розумних») взаємопов'я-

заних транспортних засобів, «розумних» будівель) розглядають вимоги до передавання безлічі різномасштабних неоднорідних даних, для чого треба будувати ефективні стратегії математичного моделювання даних, що вимірюються. У [18] розглянуто ці актуальні проблеми і описано низку методологій проектування, які використовують для відомих функцій в автономному IoT (інтелектуальна гірничо-промисловість, розумне надійне зондування, замкнений (мережевий) контроль і енергоефективність).

Під час моделювання інтернету речей, на думку авторів [19], виникають дві основні проблеми, що пов'язані з масштабуванням та високим рівнем деталізації. Технічні рішення, що дозволяють уникнути цих проблем, знаходяться у протиріччі. У цій роботі представлено огляд існуючих методів моделювання та на основі проведеного аналізу запропоновано використання адаптивного, агентного, паралельного та розподіленого моделювання у поєднанні з багаторівневим та гібридним підходами. Моделювання IoT дозволяє оцінювати стратегії розгортання інтелектуальних послуг на різних типах територій імітованих областей.

Пристрої IoT обмежені ресурсами і не можуть використовувати традиційні схеми розподілу ключів. Як наслідок зростає інтерес до локальної генерації секретних випадкових ключів з використанням спільної випадковості комунікаційного каналу. У [20] представлено схему генерації секретних ключів SKYGlow, яка орієнтована на платформи IoT з обмеженими ресурсами та тестується на пристроях, що мають радіостанції IEEE 802.15.4.

Для розв'язання практичних завдань та проблем у [21] розглянуто численні методи аналізу даних IoT. Запропоновано враховувати три факти під час застосування аналітичних алгоритмів до інтелектуальних даних. По-перше, різні застосовні програми в IoT і розумних містах мають свої особливості, такі як кількість пристроїв і типів даних, які вони генерують. По-друге, отримані дані матимуть специфічні особливості, які слід враховувати. По-третє, таксономія алгоритмів є ще одним важливим аспектом у застосуванні аналізу до розумних даних. Аналітичні дані дозволяють легко вибрати відповідний алгоритм для розв'язання конкретної проблеми.

Ґрунтовний аналіз масивних аналітичних даних щодо гетерогенного, нелінійного, високовимірного, розподіленого та паралельного їхнього оброблення було проведено в [22]. Тут запропоновано систематичні вказівки для розроблення ефективних алгоритмів аналізу Big Data в IoT. Алгоритми згруповані у чотири класи: обробка різноманітних даних; нелінійна обробка даних; обробка багатовимірних даних; розподілена та паралельна обробка даних.

У [23] представлено широкий огляд методів дослідження операцій для аналізу IoT. У роботі проаналізовано 144 публікації та проведено систематизацію використаних під час моделювання IoT методів та підходів.

Зауважимо, що в роботах [2, 8–11, 13, 15, 17, 19] використання математичних методів здебільшого анонсується, але конкретні математичні формули та розрахунки не наведено.

В табл. 1 розміщено систематизовану інформацію щодо математичних теорій, методів та моделей, використаних у проаналізованих роботах, а саме вказано мету та основні завдання, які ставили перед собою автори згаданих робіт, та зазначено перспективи подальших досліджень.

Таблиця 1

Номер джерела	Математичний апарат	Мета моделювання (основне завдання)	Перспективи подальших досліджень
1	2	3	4
[1]	Булева алгебра, матрична алгебра, експертне оцінювання, теорія ймовірностей	Розробити структурну та функціональну декомпозицію системи фізичної безпеки; знайти прикладні рішення для реалізації структурних функцій підсистем у системі фізичної безпеки; проаналізувати теоретико-множинну модель компонентів, середовища і системи фізичної безпеки	З огляду на те, що модель описує статичну ситуацію, для дослідження динамічної моделі запропоновано розглянути ситуацію атаки
[3]	Теорія ймовірностей, теорія графів	Створити модель споживання енергії в системах IoT та в пристроях, що є їхніми складовими, для підвищення енергоефективності (модель проілюстровано на прикладі системи управління будівлями)	Дистанційне керування в будівлі та його вплив на загальне споживання енергії
[4]	Теорія чисел, теорія функцій комплексної змінної, теорія ймовірностей та математична статистика, матрична алгебра	Побудувати алгоритми оцінювання каналів з підтримкою NDMRS та перевірити їхню ефективність щодо швидкості бітових помилок, пов'язаної зі співвідношенням сигнал–шум	Аналізування зміщення несучої частоти і рознесення приймача для покращення продуктивності систем NB-IoT
[5]	Теорія міри, теорія оптимізації	Розробити модель споживання енергії широкомовної мережі (для врахування споживання енергії радіостанції розглянуто чотири основні компоненти енергоспоживання: оптичний приймач, модулятор, підсилювач високої потужності і охолодження)	Емуляція динамічної мережі мовлення з циклом зворотного зв'язку IoT з реальним сценарієм
[6]	Теорія графів, теорія множин, кластерний аналіз	Побудувати два алгоритми кластеризації на основі евристичного методу та теорії графів (запропоновані підходи кластеризації оцінюють на платформі IoT за допомогою стандартних параметрів і порівнюють з різними підходами)	Розширення запропонованого алгоритму підключенням до хмари IoT; збільшення кількості параметрів моделі та визначення характеристик евристичних чи графних ребер для кластеризації залежно від застосування
[7]	Імітаційне моделювання, теорія ймовірностей	Побудувати правдоподібну імітаційну модель для прогнозування скачків трафіку	Поглиблене аналізування отриманих даних, необхідне для побудови імітаційної моделі мережі пристроїв IoT з подальшими ускладненнями і збільшенням кількості вузлів
[12]	Теорія графів	Провести оцінювання продуктивності семантичної моделі онтології, розробленої оперативно-операційними службами	Подолання монолітних підходів, мікросервісів, що можуть самостійно створювати нові функції обслуговування

1	2	3	4
[14]	Теорія оптимізації	Мінімізувати негативні наслідки кібератак	Подолання вкрай небажаних можливостей самоорганізуватися в мережі для забезпечення віртуалізованого, багатостороннього IoT-трафіку на основі 5G
[16]	Теорія ймовірностей, математична статистика, теорія випадкових процесів, імітаційне моделювання, чисельний аналіз	Провести оцінювання часових характеристик інформаційної взаємодії в мережі IoT. Знайти залежність часових характеристик від параметрів мережі IoT	Розрахування виразів, алгоритмів і моделей, необхідних на ранніх етапах проектування мережі інтернету речей
[18]	Теорія випадкових процесів, теорія оптимізації	Розробити методологію проєктування, яку використовують для функцій в автономному IoT	Створення енергоефективної, надійної та інтегрованої системи IoT
[20]	Теорія ймовірностей, теорія випадкових процесів, теорія оптимізації	Розв'язати проблему розподілу та декількох важливих функціональних особливостей та обмежень для IoT з обмеженими ресурсами	Покращання роботи запропонованого алгоритму глобальної оптимізації, який працює нарівні з комерційними рішеннями, але не такий швидкий, як евристичний підхід
[21]	Теорія ймовірностей, теорія графів, теорія оптимізації	Розробити алгоритм зміни повідомлення для надійності збереження інформації	Встановлення криптографічно захищених зв'язків між пристроями IoT, що вимагає попереднього консенсусу з секретним ключем шифрування
[22]	Математичний аналіз, теорія оптимізації	Побудувати алгоритми для аналітики Big Data	Розроблення практичних та ефективних алгоритмів для конкретних застосовних програм IoT, для забезпечення розумного розподілу ресурсів, автоматичного функціонування мережі та інтелектуального надання послуг
[23]	Теорія ігор, теорія графів	Проаналізувати математичні методи і моделі IoT	Знаходження балансу між проблемами технічних і нетехнічних досліджень

Останнім часом термін IoT та англomовний прикметник «смарт» досить часто використовують в українській мові. Кількість пристроїв, що фіксують відповідну інформацію, зростає в рази, а об'єм даних, що генерують розумні пристрої, збільшився на порядки. Зрозуміло, що для проведення аналізу, ефективного функціонування та прогнозування роботи складної системи інтернету речей необхідним є використання математичних методів та моделей. Це передбачає достатній рівень теоретичних знань з певних дисциплін математичного циклу. У статті представлено огляд публікацій останніх років щодо використання мате-

матричних методів та моделей для проведення аналізу IoT. Показано, що під час моделювання IoT використовують такі розділи математики, як теорія ігор, теорія ймовірностей, теорія випадкових процесів, булева та матрична алгебра, теорія графів, теорія чисел, теорія функції комплексної змінної, теорія міри, теорія оптимізації, імітаційне моделювання, кластерний аналіз, чисельний аналіз, математичний аналіз. Ця робота буде корисною для науковців, практиків, що цікавляться IoT, та для викладачів вищих навчальних закладів, що ведуть підготовку фахівців зі спеціальності «Інформаційні технології».

СПИСОК ЛІТЕРАТУРИ

1. Аль-Хафаджі Ахмед Валід. Розроблення методики PSMECA аналізу при застосуванні IoT компонентів у системах фізичної безпеки. *Радіоелектронні і комп'ютерні системи*. 2018. № 3(87). С. 63–73. <http://doi.org/10.32620/reks.2018.3.07>.
2. Тарасов О. Ф., Турлакова С.С. Математическое моделирование передовых машиностроительных технологий для smart-предприятий: обзор подходов и пути внедрения. *Экономика промышленности*. 2018. № 3(83). С. 57–75. <http://doi.org/10.15407/econindustry2018.03.057>.
3. Lekidis A., Katsaros P. Model-based design of energy-efficient applications for IoT systems. Bliudze S., Bensalem S. (Eds.). *Methods and Tools for Rigorous System Design (MeTRiD 2018) EPTCS 272*. 2018. P. 24–38. <http://doi.org/10.4204/EPTCS.272.3>.
4. Md Sadek Ali, Li Yu, Md Khalid Hossain Jewel, Oluwole John Famoriji, Fujiang Lin. Channel estimation and peak-to-average power ratio analysis of narrowband internet of things uplink systems. *Hindawi. Wireless Communications and Mobile Computing*. 2018. Vol. 2018. Article ID 2570165. 15 p. <https://doi.org/10.1155/2018/2570165>.
5. Alonso R.M., Plets D., Pupo E.F., Deruyck M., Martens L., Nieto G.G., Joseph W. IoT-based management platform for real-time spectrum and energy optimization of broadcasting networks. *Hindawi. Wireless Communications and Mobile Computing*. 2018. Vol. 2018. Article ID 7287641. 14 p. <https://doi.org/10.1155/2018/7287641>.
6. J. Sathish Kumar, Mukesh A. Zaveri. Clustering approaches for pragmatic two-layer IoT architecture. *Hindawi. Wireless Communications and Mobile Computing*. 2018. Vol. 2018. Article ID 8739203. 16 p. <https://doi.org/10.1155/2018/8739203>.
7. Лоднева О.Н., Ромасевич Е.П. Анализ трафика устройств Интернета вещей. *Современные информационные технологии и ИТ-образование*. 2018. Т. 14, № 1. С. 149–169. <http://doi.org/10.25559/SITITO.14.201801.149-169>.
8. Турлакова С.С. Информационно-коммуникационные технологии развития «умных» производств. *Экономика промышленности*. 2019. № 1(85). С. 101–123. <https://doi.org/10.15407/econindustry2019.01.101>
9. Mohamed S., Khalid E., Kasem K. Towards privacy preserving IoT environments: A survey. *Hindawi. Wireless Communications and Mobile Computing*. 2018. Vol. 2018. Article ID 1032761. 15 p. <https://doi.org/10.1155/2018/1032761>.
10. Triantafyllou A., Sarigiannidis P., Lagkas T.D. Network protocols, schemes, and mechanisms for internet of things (IoT): Features, open challenges, and trends. *Hindawi. Wireless Communications and Mobile Computing*. 2018. Vol. 2018. Article ID 5349894. 24 p. <https://doi.org/10.1155/2018/5349894>.
11. Maruf Pasha and Syed Muhammad Waqas Shah. Framework for E-health systems in IoT-based environments. *Hindawi. Wireless Communications and Mobile Computing*. 2018. Vol. 2018. Article ID 6183732. 11 p. <https://doi.org/10.1155/2018/6183732>.
12. Sajjad Ali, Muhammad Golam Kibria, Muhammad Aslam Jarwar, Hoon Ki Lee, and Ilyoung Chong. A model of socially connected web objects for IoT applications. *Hindawi. Wireless Communications and Mobile Computing*. 2018. Vol. 2018. Article ID 6309509. 20 p. <https://doi.org/10.1155/2018/6309509>.
13. Junwoo Seo, Kyoungmin Kim, Mookyu Park, Moosung Park, and Kyungho Lee. An analysis of economic impact on IoT industry under GDPR. *Hindawi. Mobile Information Systems*. 2018. Vol. 2018. Article ID 6792028. 6 p. <https://doi.org/10.1155/2018/6792028>
14. Salva-Garcia P., Alcaraz-Calero J.M., Wang Q., Bernabe J.B., Skarmeta A. 5G NB-IoT: Efficient network traffic filtering for multitenant IoT cellular networks. *Hindawi. Security and Communication Networks*. 2018. Vol. 2018. Article ID 9291506. 21 p. <https://doi.org/10.1155/2018/9291506>.

15. Sufian Hameed, Faraz Idris Khan, Bilal Hameed. Understanding security requirements and challenges in internet of things (IoT): A review. *Hindawi. Journal of Computer Networks and Communications*. 2019. Vol. 2019. Article ID 9629381. 14 p. <https://doi.org/10.1155/2019/9629381>.
16. Елезаров М.А. Модели и алгоритмы информационного взаимодействия в сетях Интернета вещей. Автореф. дис. ... канд. техн. наук. СПб., 2017. 18 с.
17. Breiner S., Subrahmanian E., Sriram R.D. Modeling the internet of things: A foundational approach. *WoT'16 Proceedings of the Seventh International Workshop on the Web of Things*. (Stuttgart, Germany. November 07.07.2016). P. 38–41. <http://doi.org/10.1145/3017995.3018003>.
18. Bogdan P., Pajic M., Pande P.P., Raghunathan V. Making the Internet-of-things a reality: from smart models, sensing and actuation to energy-efficient architectures. *CODES'16 Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis*. (Pittsburgh, Pennsylvania. October 01.07.2016). Article N 25. <https://doi.org/10.1145/2968456.2973272>.
19. D'Angelo G., Ferretti S., Ghini V. Modeling the Internet of things: A simulation perspective. URL: <https://arxiv.org/abs/1707.00832v2>. <https://doi.org/10.1109/HPCS.2017.13>.
20. Margelis G., Fafoutis X., Oikonomou G., Piechocki R., Tryfonas T., Thomas P. Efficient DCT-based secret key generation for the Internet of things. *Ad Hoc Networks* 92 (2019) 101744, P. 1–11.
21. Mohammad Saeid Mahdavejad, Mohammadreza Rezvan, Mohammadamin Barekatin, Peyman Adibi, Payam Barnaghi, Amit P. Sheth. Machine learning for internet of things data analysis: a survey. *Digital Communications and Networks*. 2018. N 4. P. 161–175.
22. Guoru Ding, Long Wang, Qihui Wu. Big data analytics in future Internet of things. URL: <https://arxiv.org/abs/1311.4112>.
23. Ryan P.J., Watson R.B. Research challenges for the Internet of things: What role can or play? *Systems*. 2017. 5. 24. <http://doi.org/10.3390/systems5010024>.

Надійшла 26.10.2019

А.В. Мамонова, Н.В. Майданюк

МАТЕМАТИЧЕСКИЙ ИНСТРУМЕНТАРИЙ ДЛЯ АНАЛИЗА ИНТЕРНЕТА ВЕЩЕЙ

Аннотация. Представлен обзор публикаций последних лет об использовании математических методов и моделей для анализа интернета вещей. Отмечено, что при моделировании интернета вещей используются такие разделы математики, как теория игр, теория вероятностей, теория случайных процессов, булева и матричная алгебра, теория графов, теория чисел, теория функции комплексного переменного, теория меры, теория оптимизации, имитационное моделирование, кластерный анализ, численный анализ, математический анализ.

Ключевые слова: интернет вещей, методы, модели, моделирование, технологии, структура, система.

G. Mamonova, N. Maidaniuk

MATHEMATICAL INSTRUMENTS FOR ANALYSIS OF THE INTERNET OF THINGS

Abstract. The analysis of recent years' publications on the use of mathematical methods and models for IoT analysis is presented. The analysis showed that the authors use sections of mathematics such as game theory, probability theory, theory of random processes, Boolean and matrix algebra, graph theory, number theory, theory of function of complex variable, theory of measure, theory of optimization, theory of optimization analysis, numerical analysis, and mathematical analysis.

Keywords: Internet of Things, methods, models, modeling (simulation), technology, structure, system.

Мамонова Ганна Валеріївна,

кандидат фіз.-мат. наук., доцент кафедри Державного вищого навчального закладу «Київський національний економічний університет імені Вадима Гетьмана», e-mail: mamonova@kneu.edu.ua.

Майданюк Надія Володимирівна,

аспірантка, Міжнародного науково-навчального центру інформаційних технологій та систем НАН та МОН України, Київ, e-mail: n.maydanyuk@ukr.net.